II. AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of protecting security of a network server from unauthorized content contained in a message received for processing by said server from a user, the method comprising:

intercepting said message that includes information entered for constructing a query to access data of the server before any content of said message is processed by said server, the message including the information for constructing the query that includes an entirety of a string of text based information entered by a user into a web page provided by the server directly incorporated therein;

examining said message to determine if it contains one or more unauthorized elements, the examining comprising:

receiving an identification of an execution program set to be used to process said message received, the execution program set being a set of routines that incorporate data entered by a user in a particular execution page into a database query for a particular database;

retrieving an identification of all message types associated with said execution program set, wherein the message types are based on a structure of elements in a database query and are chosen from the group consisting of: single token; string; multiple tokens without keywords: OR, UNION and SEMI-COLON; multiple tokens without keywords:

UNION and SEMI-COLON; multiple tokens without keywords: SEMI-COLON; and multiple tokens without restriction;

examining said message received by said server in relation to said message types associated with said execution program set; and

determining if said message received by said server contains an unauthorized element in relation to the corresponding message type for said message received;

if it is determined that said message contains an unauthorized element preventing said message received from being processed by said server;

if it is determined that said message does not contain an unauthorized element allowing said message received to be processed by said server.

2. (Original) The method of claim 1 wherein, if it is determined that said message received contains an unauthorized element, preventing said message received from being processed by said server, and causing an error notification to be sent to said user.

3. (Cancelled).

4. (Previously Presented) The method of claim 1 wherein, if it is determined that said message received contains an unauthorized element, causing an error notification to be sent to said user.

5. (Currently Amended) A method of protecting security of an Internet network server from unauthorized content contained in a message received over the Internet by said server from a user, the method comprising:

intercepting said message that includes information for constructing a query to access data of the server before any content of said message is processed by said server, the message including the information for constructing the query that includes an entirety of a string of text based information entered by a user into a web page provided by the server directly incorporated therein;

examining said message to determine if it contains one or more unauthorized elements, the examining comprising:

receiving an identification of an execution program set to be used to process said message received, the execution program set being a set of routines that incorporate data entered by a user in a particular execution page into a database query for a particular database;

retrieving an identification of all message types associated with said execution program set, wherein the message types are based on a structure of elements in a database query and are chosen from the group consisting of: single token; string; multiple tokens without keywords: OR, UNION and SEMI-COLON; multiple tokens without keywords: UNION and SEMI-COLON; multiple tokens without keywords: SEMI-COLON; and multiple tokens without restriction;

examining said message received by said server in relation to said message types associated with said execution program set; and

determining if said message received by said server contains an unauthorized element in relation to a corresponding message type for said message received;

if it is determined that said message contains an unauthorized element, preventing said message received from being processed by said server;

if it is determined that said message received does not contain an unauthorized element, allowing said message received to be processed by said server.

6. (Original) The method of claim 5 wherein, if it is determined that said message received contains an unauthorized element preventing said message received from being processed by said server, causing an error notification to be sent to said user.

7. (Cancelled).

8. (Previously Presented) The method of claim 5 wherein, if it is determined that said message received contains an unauthorized element, causing an error notification to be sent to said user.

9. (Original) The method of claim 8 wherein, if it is determined that said message received does not contain an unauthorized element, allowing said message received to be processed by said server.

10. (Previously Presented) The method of claims 1 or 5, wherein said message comprises a name-value pair.

11. (Original) The method of claim 10 wherein said element comprises one or more of the following items: an instruction, a command, a character, a parameter, a token, or a string of any of said previous items.

12. (Original) The method of claims 11 wherein said element is interpretable as an instruction or command by said server.

13. (Currently Amended) Security control apparatus for controlling the security of a network server from unauthorized content contained in a message received from a user of said server, the apparatus comprising:

at least one computing device, including;

means for intercepting said message received that includes information for constructing a query to access data of the server before any content of said message is processed by said server, the message including the information for constructing the query that includes an entirety of a string of text based information entered by a user into a web page provided by the server directly incorporated therein;

means for examining said message received to determine if it contains one or more unauthorized elements, the means for examining further comprising:

means for receiving an identification from said user of an execution program set retrievable by said server to be used to process said message received, the execution program set being a set of routines that incorporate data entered by a user in a particular

execution page into a database query for a particular database;

means for retrieving an identification of message types associated with said execution program set from facilities associated with said server, wherein the message types are based on a structure of elements in a database query and are chosen from the group consisting of: single token; string; multiple tokens without keywords; OR, UNION and SEMI-COLON; multiple tokens without keywords: UNION and SEMI-COLON; multiple tokens without keywords: SEMI-COLON; and multiple tokens without restriction;

means for examining said message received by said server in relation to said message types associated with said execution program set; and

means for determining if said message received by said server contains an unauthorized element in relation to a corresponding message type for said message received;

means for preventing said message received from being processed by said server if it is determined that said message received contains an unauthorized element;

means for allowing said message received to be processed by said server if it is determined that said message received does not contain an unauthorized element.

14. (Previously Presented) The apparatus of claim 13 wherein said network server comprises an Internet network server and said message is received over the Internet by said server from a user.

15. (Original) The apparatus of claim 13 or 14 further comprising means for returning an error message to said user.

16. (Cancelled).

17. (Cancelled).

18. (Previously Presented) The apparatus of claim 13 wherein said message comprises a name-value pair and said element is contained by said name-value pair.

19. (Original) The apparatus of claim 18 wherein said element comprises one or more of the following items: an instruction, a command, a character, a parameter, a token, or a string of any of said previous items.

20. (Original) The apparatus of claim 19 wherein said element is interpretable as an instruction or command by said server.

21-23. (Canceled).

24. (Previously Presented) The method of claim 1, wherein the query is a database query that includes an entirety of the information entered by the user into a field of the web page.